8T

УДК 510.52

А.Н. Терещенко, В.К. Задирака, А.М. Кудин
Институт кибернетики имени В.М. Глушкова НАН Украины, г. Киев, Украина
teramidi@ukr.net, zvk140@ukr.net

Использование циклических сдвигов для ускоренного вычисления циклических сверток длины равной произведению взаимно простых чисел

В работе рассматривается метод вычисления циклических сверток длины $N = \prod_{i=0}^{n-1} m_i$, где $(m_i, m_j) = 1$, $i \neq j$. Рассматривается новое блочно-циклическое представление свертки за счет использования циклических сдвигов в каждом блоке. При таком подходе китайская теорема об остатках (КТО) не используется. Метод является эффективным за счет использования несложных пред- и поствычислений с применением циклических сдвигов. Он позволяет распараллелить вычисления. Получены априорные оценки сложности по количеству операций умножения. Приведены примеры вычислений сверток.

Введение

Циклические свертки широко используются при построении цифровых фильтров, в задачах ассиметричной криптографии и т.д. Как известно, выбор метода зависит от области его эффективного использования. Циклическая свертка используется при реализации быстрой операции умножения с использованием быстрых преобразований Фурье, Уолша, Хаара [1]. Операция умножения занимает большую часть вычислительного времени при реализации операций ассиметричной криптографии, в частности в задачах распространения секретного ключа, шифрования информации, выработки и верификации электронно-цифровой подписи и т.д.

В работе [2] Д. Питасси предложил метод вычисления циклической свертки длины $N = 2^n$, усовершенствованный впоследствии Девисом [3]. Данный метод приводит операцию вычисления циклической свертки длины 2^n к вычислению трех циклических сверток половинной длины 2^{n-1}. На каждой итерации количество сверток половинной длины увеличивается в три раза. Итерации продолжаются до получения сверток длины 2. В работе [4], следуя Питасси, показано, что вычисление циклической свертки длины $N = 2 \cdot k$, k – нечетное, сводится к вычислению двух сверток длины k, что позволяет реализовать операцию умножения двух k-разрядных чисел, k – нечетное. Метод, рассматриваемый в данной работе, является продолжением работы [4]. В работе [5] приведен метод умножения больших чисел, основанный на циклической свертке длиной, равной степени двойки с использованием преобразования Уолша. В работе [6] приведены оптимальные алгоритмы по количеству операций умножения, сложения и вычитания для вычисления сверток длины 2, 3, 4, 5, 7, 8, 9. Р.К. Агарвал и Ч.С. Баррас предложили отображать одномерный массив в многомерный, используя удвоение числа точек [7]. В работе Винограда [8] для

вычисления длинных сверток применяются билинейные формы. В работе [9] Р.К. Агарвал и Дж.У. Кули применяют китайскую теорему об остатках (КТО) для преобразования одномерной циклической свертки в многомерную, которая циклична по всем направлениям. Упомянутые выше работы направлены на уменьшение числа однословных умножений. Сегодня архитектура современного процессора такова, что операции однословного умножения и сложения выполняются за одинаковое число тактов. Поэтому дальнейшие работы должны учитывать этот факт и также быть направлены на оптимизацию количества таких однословных операций, как сложение, вычитание, сдвиги. Одним из оригинальных подходов для решения таких задач можно назвать комбинацию программного и аппаратного подхода, при котором перед началом каждого вычисления в зависимости от длины входных данных прошиваются эффективные для данных длин подпрограммы [10].

Для вычисления свертки длины N стандартным методом необходимо выполнить N^2 операций умножения, что соответствует умножению квадратной матрицы на вектор длины N. Продолжая идею Питасси [2], [3], операцию вычисления циклической свертки длины $N=15$ ($r_j=\sum_{m=0}^{N-1} x_m \cdot y_{\langle m+j\rangle_N}$, $j=\overline{0, N-1}$) можно свести к вычислению трёх сверток длины $N=5$ (рис. 1).

y_0	x_0	x_{12}	x_9	x_6	x_3	x_5	x_2	x_{14}	x_{11}	x_8	x_{10}	x_7	x_4	x_1	x_{13}
y_3	x_3	x_0	x_{12}	x_9	x_6	x_8	x_5	x_2	x_{14}	x_{11}	x_{13}	x_{10}	x_7	x_4	x_1
y_6	x_6	x_3	x_0	x_{12}	x_9	x_{11}	x_8	x_5	x_2	x_{14}	x_1	x_{13}	x_{10}	x_7	x_4
y_9	x_9	x_6	x_3	x_0	x_{12}	x_{14}	x_{11}	x_8	x_5	x_2	x_4	x_1	x_{13}	x_{10}	x_7
y_{12}	x_{12}	x_9	x_6	x_3	x_0	x_2	x_{14}	x_{11}	x_8	x_5	x_7	x_4	x_1	x_{13}	x_{10}
y_{10}	x_{10}	x_7	x_4	x_1	x_{13}	x_0	x_{12}	x_9	x_6	x_3	x_5	x_2	x_{14}	x_{11}	x_8
y_{13}	x_{13}	x_{10}	x_7	x_4	x_1	x_3	x_0	x_{12}	x_9	x_6	x_8	x_5	x_2	x_{14}	x_{11}
y_1	x_1	x_{13}	x_{10}	x_7	x_4	x_6	x_3	x_0	x_{12}	x_9	x_{11}	x_8	x_5	x_2	x_{14}
y_4	x_4	x_1	x_{13}	x_{10}	x_7	x_9	x_6	x_3	x_0	x_{12}	x_{14}	x_{11}	x_8	x_5	x_2
y_7	x_7	x_4	x_1	x_{13}	x_{10}	x_{12}	x_9	x_6	x_3	x_0	x_2	x_{14}	x_{11}	x_8	x_5
y_5	x_5	x_2	x_{14}	x_{11}	x_8	x_{10}	x_7	x_4	x_1	x_{13}	x_0	x_{12}	x_9	x_6	x_3
y_8	x_8	x_5	x_2	x_{14}	x_{11}	x_{13}	x_{10}	x_7	x_4	x_1	x_3	x_0	x_{12}	x_9	x_6
y_{11}	x_{11}	x_8	x_5	x_2	x_{14}	x_1	x_{13}	x_{10}	x_7	x_4	x_6	x_3	x_0	x_{12}	x_9
y_{14}	x_{14}	x_{11}	x_8	x_5	x_2	x_4	x_1	x_{13}	x_{10}	x_7	x_9	x_6	x_3	x_0	x_{12}
y_2	x_2	x_{14}	x_{11}	x_8	x_5	x_7	x_4	x_1	x_{13}	x_{10}	x_{12}	x_9	x_6	x_3	x_0
	r_0	r_3	r_6	r_9	r_{12}	r_{10}	r_{13}	r_1	r_4	r_7	r_5	r_8	r_{11}	r_{14}	r_2

Рисунок 1 – Вычисления свертки длины $N=k\cdot r=3\cdot 5$, где k, r – нечетные

Свертки
$$\begin{matrix} x_0 & \cdots & x_3 \\ \vdots & \cdots & \vdots \\ x_{12} & \cdots & x_0 \end{matrix}, \quad \begin{matrix} x_5 & \cdots & x_8 \\ \vdots & \cdots & \vdots \\ x_2 & \cdots & x_5 \end{matrix}, \quad \begin{matrix} x_{10} & \cdots & x_{13} \\ \vdots & \cdots & \vdots \\ x_7 & \cdots & x_{10} \end{matrix}$$
повторяются по три раза.

Данный подход позволяет значительно уменьшить число операций умножения, сложения, вычитания и т.д.

Далее будет показано, что вычисление любой циклической свертки длины $N = k \cdot r$, $(k, r) = 1$, $k < r$, можно представить в виде k блоков, повторяющихся k раз. Такой метод позволяет свести задачу вычисления свертки длины $N = k \cdot r$ к задаче вычисления свертки длины k. Далее будем использовать выражение «секция» вместо «блок», что созвучно с методом парисекции, рассмотренным Девисом [3].

Новизной предложенного метода является использование циклических сдвигов в каждом блоке для представления свертки в блочно-циклическом виде без использования китайской теоремы об остатках. Преимуществом данного метода является то, что не используются предвычисления, на каждой итерации достаточно знать p ($N = k \cdot r$, $k < r$, $d = r - k$, $\langle p \cdot d \rangle_r = 1$), не используются дискретные преобразования, метод разбиения подобный для любых длин сверток.

Операторы и обозначения

Перед тем как рассмотреть предложенный метод, введем следующие операторы и обозначения. Последовательности X_N и Y_N длины N представляются векторами-столбцами:

$$X_N = \begin{bmatrix} x_0 \\ \vdots \\ x_{N-1} \end{bmatrix}, \; Y_N = \begin{bmatrix} y_0 \\ \vdots \\ y_{N-1} \end{bmatrix}.$$

Циклическую свертку двух сигналов X_N и Y_N обозначим оператором $\otimes$:

$$R_N = X_N \otimes Y_N, \; R_N = \begin{bmatrix} r_0 \\ \vdots \\ r_{N-1} \end{bmatrix}, \; r_k = \sum_{m=0}^{N-1} x_m y_{\langle m+j \rangle_N}, \; j = \overline{0, N-1},$$

что соответствует записи:

$$\begin{array}{c|cccc} x_0 & y_0 & y_1 & y_2 & y_3 \\ x_1 & y_1 & y_2 & y_3 & y_0 \\ x_2 & y_2 & y_3 & y_0 & y_1 \\ x_3 & y_3 & y_0 & y_1 & y_2 \\ \hline & r_0 & r_1 & r_2 & r_3 \end{array} \quad \text{или} \quad \begin{array}{c|cccc} y_0 & x_0 & x_3 & x_2 & x_1 \\ y_1 & x_1 & x_0 & x_3 & x_2 \\ y_2 & x_2 & x_1 & x_0 & x_3 \\ y_3 & x_3 & x_2 & x_1 & x_0 \\ \hline & r_0 & r_1 & r_2 & r_3 \end{array}.$$

Введем следующие операторы: S, P, U, D (*S*-“*Select*” (выбрать), *P*-“*Part*” (часть), *U*-“*Up*” (вверх), *D*-“*Down*” (вниз)), и обозначим их следующим образом:

$$S_{i,j}^r X_N = x_{i+j \cdot k}, \; j = \overline{0, r-1}, \; i = \overline{0, k-1}, \text{ где } k = N/r;$$

циклический сдвиг элементов вверх – $V_N = UX_N$, $v_k = x_{\langle k+1 \rangle_N}$, $k = \overline{0, N-1}$;

циклический сдвиг элементов вниз – $V_N = DX_N$, $v_k = x_{\langle k+N-1 \rangle_N}$, $k = \overline{0, N-1}$;

циклический сдвиг элементов вверх p раз – $V_N = U^p(X_N)$, $v_k = x_{\langle k+p \rangle_N}$, $k = \overline{0, N-1}$;

циклический сдвиг элементов вниз p раз – $V_N = D^p(X_N)$, $v_k = x_{\langle k+N-p \rangle_N}$, $k = \overline{0, N-1}$.

Проиллюстрируем операторы для длин $N = 5, 12, 15$:

$$DX_5 = \begin{bmatrix} x_4 \\ x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix},\ UX_5 = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_0 \end{bmatrix},\ D^2(X_5) = \begin{bmatrix} x_3 \\ x_4 \\ x_0 \\ x_1 \\ x_2 \end{bmatrix},\ U^2(X_5) = \begin{bmatrix} x_2 \\ x_3 \\ x_4 \\ x_0 \\ x_1 \end{bmatrix},$$

$$U^3(S_4^0 X_{12}) = \begin{bmatrix} x_9 \\ x_0 \\ x_3 \\ x_6 \end{bmatrix} = D^1(S_4^0 X_{12}),$$

$$S_5^0 X_{15} = \begin{bmatrix} x_0 \\ x_3 \\ x_6 \\ x_9 \\ x_{12} \end{bmatrix},\ S_5^1 X_{15} = \begin{bmatrix} x_1 \\ x_4 \\ x_7 \\ x_{10} \\ x_{13} \end{bmatrix},\ S_5^2 X_{15} = \begin{bmatrix} x_2 \\ x_5 \\ x_8 \\ x_{11} \\ x_{14} \end{bmatrix},\ P_5^0 X_{15} = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix},\ P_5^1 X_{15} = \begin{bmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \end{bmatrix},$$

$$P_5^2 X_{15} = \begin{bmatrix} x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \end{bmatrix}.$$

Постановка задачи. Если целые положительные векторы X_N, Y_N, R_N вида $X_N = \sum_{i=0}^{N-1} x_i 2^{\omega i}$, $Y_N = \sum_{i=0}^{N-1} y_i 2^{\omega i}$, $R_N = \sum_{i=0}^{N-1} r_i 2^{\omega i}$, где $0 \le x_i, y_i, r_i < 2^{\omega}$, $N = 2^{\gamma}$, тогда выражение R_N вида

$$R_N = X_N \otimes Y_N = \left(\sum_{i=0}^{N-1} x_i 2^{\omega i} \right) \otimes \left(\sum_{i=0}^{N-1} y_i 2^{\omega i} \right) = \sum_{\tau=0}^{N-1} r_\tau 2^{\omega \tau},$$

где $r_\tau = \sum_{\rho+\delta=\tau (\mathrm{mod}\, N)} x_\rho \cdot y_\delta$, представляет собой циклическую свертку X_N и Y_N. Необходимо найти эффективный алгоритм вычисления циклической свертки.

Свойства последовательностей

Лемма 1. Пусть последовательность J_N составляют элементы $j = \overline{0, N-1}$, где $N = k \cdot r$, $k < r$, $(k, r) = 1$. Если J_N разбить на k секций длины r с использованием оператора S, то каждая секция $S_r^i J_N$, $i = \overline{0, k-1}$, содержит индекс, которой делится на r.

Доказательство. Так как каждая секция является результатом применения оператора S, то соседние элементы внутри каждой секции отличаются на k. Нулевая секция $i = 0$ будет состоять из следующих элементов:

$$0, k, 2k, \ldots, (r-1) \cdot k.$$

Элементы секции $i=1$ будут следующими:

$$1, 1+k, 1+2k, ..., 1+(r-1)\cdot k .$$

Их можно выразить следующим образом:

$$z = 1 + p\cdot k ,\ p = \overline{0, r-1} , \qquad (1)$$

где r – длина секции.

Найдем значение p, при котором z делится на r без остатка.

Сделаем замену $k = r - d$ в формуле:

$$z = \langle 1 + p\cdot k\rangle_N = \langle 1 + p\cdot(r-d)\rangle_N = \langle 1 + p\cdot r - p\cdot d\rangle_N = \langle p\rangle_k \cdot r + \langle 1 - p\cdot d\rangle_N ,\ p = \overline{0, N-1} .$$

Отсюда видно, что z будет делиться на r только в том случае, когда $\langle 1 - p\cdot d\rangle_{N=k\cdot r}$ делится на r: $\langle 1 - p\cdot d\rangle_r = 0$, $1 = \langle p\cdot d\rangle_r = \langle d^{-1}\cdot d\rangle_r$, т.е. когда $p = d^{-1}$. Число p можно найти, используя расширенный алгоритм Эвклида:

$$d\cdot p - r\cdot r' = d\cdot d^{-1} - r\cdot r' = 1 ,\ r > d .$$

Для случая $i > 1$ соотношения (1) можно записать в следующем виде:

$$z_i = \langle i + (i\cdot p)\cdot k\rangle_N = \langle i\cdot(1 + p\cdot k)\rangle_N = \langle i\cdot z\rangle_N . \qquad (2)$$

С учетом того, что число секций (длины r) равно k и порядковый номер в секции не может превышать длины секции $(i\cdot p) < r$, соотношение (2) примет следующий вид:

$$z = 1 + p\cdot k ;\ z_i = \langle i + p_i\cdot k\rangle_N = \langle i\cdot z\rangle_N ,\ p_i = \langle i\cdot p\rangle_r ,\ i = \overline{0, k-1} , \qquad (3)$$

где k – количество секций длины r, p – порядковый номер элемента в секции i со значением z_i, которое делится на r без остатка.

Окончательно получаем:

$$p = d^{-1} = \langle (r-k)^{-1}\rangle_r ;\ p_i = \langle i\cdot p\rangle_r ,\ i = \overline{0, k-1} . \qquad (4)$$

$$z = 1 + p\cdot k ;\ z_i = \langle i\cdot z\rangle_N ,\ i = \overline{0, k-1} . \qquad (5)$$

Лемма доказана.

Соотношение (5) можно представить в виде $z_i = r\cdot\langle i\cdot z/r\rangle_k$, $i = \overline{0, k-1}$, упрощающем вычисление z_i.

Лемма 1 устанавливает зависимость между числом циклических сдвигов p секции, номером секции i, числом секций k и длиной секции r.

Для примера рассмотрим последовательность $J_{15} = (0, 1, ..., 14)$, $N = 15$, $k = 3$, $r = 5$. Вычислим $p = d^{-1} = \langle (r-k)^{-1}\rangle_r = \langle 2^{-1}\rangle_5 = 3$, $z = 1 + 3\cdot 3 = 10$. Найдем p_i, z_i, $i = \overline{0, k-1} = \overline{0, 2}$, используя соотношение (3).

Таблица 1 – Вычисление $S_r^i J_N$, $p_i = \langle i\cdot p\rangle_r$, $z_i = \langle i\cdot z\rangle_N$, $i = \overline{0, k-1}$, для $N = k\cdot r = 3\cdot 5 = 15$, где k, r – нечетные

i	$S_r^i J_N$	$p_i = \langle i\cdot p\rangle_r$	$z_i = \langle i\cdot z\rangle_N$
$i=0$	$S_5^0 J_{15} = (0, 3, 6, 9, 12)$	$p_0 = \langle 0\cdot 3\rangle_5 = 0$	$z_0 = \langle 0\cdot 10\rangle_{15} = 0$
$i=1$	$S_5^1 J_{15} = (1, 4, 7, 10, 13)$	$p_1 = \langle 1\cdot 3\rangle_5 = 3$	$z_1 = \langle 1\cdot 10\rangle = 10$
$i=2$	$S_5^2 J_{15} = (2, 5, 8, 11, 14)$	$p_2 = \langle 2\cdot 3\rangle_5 = 1$	$z_2 = \langle 2\cdot 10\rangle_{15} = 5$

Рассмотрим $J_{35} = (0, 1, ..., 34)$, $N = 35$, $k = 5$, $r = 7$. Обратный элемент p будет равен $p = d^{-1} = \left\langle (r-k)^{-1} \right\rangle_r = \left\langle 2^{-1} \right\rangle_7 = 4$, $z = 1 + 4 \cdot 5 = 21$. Найдем p_i, z_i, $i = \overline{0, k-1} = \overline{0, 4}$, используя соотношение (3).

Таблица 2 – Вычисление $S_r^i J_N$, $p_i = \left\langle i \cdot p \right\rangle_r$, $z_i = \left\langle i \cdot z \right\rangle_N$, $i = \overline{0, k-1}$,
для $N = k \cdot r = 5 \cdot 7 = 35$, где k, r – нечетные

i	$S_r^i J_N$	$p_i = \left\langle i \cdot p \right\rangle_r$	$z_i = \left\langle i \cdot z \right\rangle_N$
$i = 0$	$S_7^0 J_{35} = (0, 5, 10, 15, 20, 25, 30)$	$p_0 = \left\langle 0 \cdot 4 \right\rangle_7 = 0$	$z_0 = \left\langle 0 \cdot 21 \right\rangle_{35} = 0$
$i = 1$	$S_7^1 J_{35} = (1, 6, 11, 16, 21, 26, 31)$	$p_1 = \left\langle 1 \cdot 4 \right\rangle_7 = 4$	$z = \left\langle 1 \cdot 21 \right\rangle_{35} = 21$
$i = 2$	$S_7^2 J_{35} = (2, 7, 12, 17, 22, 27, 32)$	$p_2 = \left\langle 2 \cdot 4 \right\rangle_7 = 1$	$z_2 = \left\langle 2 \cdot 21 \right\rangle_{35} = 7$
$i = 3$	$S_7^3 J_{35} = (3, 8, 13, 18, 23, 28, 33)$	$p_3 = \left\langle 3 \cdot 4 \right\rangle_7 = 5$	$z_3 = \left\langle 3 \cdot 21 \right\rangle_{35} = 28$
$i = 4$	$S_7^4 J_{35} = (4, 9, 14, 19, 24, 29, 34)$	$p_4 = \left\langle 4 \cdot 4 \right\rangle_7 = 2$	$z_4 = \left\langle 4 \cdot 21 \right\rangle_{35} = 14$

Анализируя табл.1, 2 и лемму 1, приходим к следующему утверждению.

Лемма 2. Пусть последовательность J_N составляют элементы $j = \overline{0, N-1}$, где $N = k \cdot r$, $k < r$, $(k, r) = 1$. Если J_N разбить на k секций длиной r с использованием оператора S, то первый элемент секций $U^{p_i} S_r^i J_N$, $i = \overline{0, k-1}$, содержит индекс z_i, которое делится на r без остатка, где p_i и z_i определяются следующими выражениями:

$$p = d^{-1} = \left\langle (r-k)^{-1} \right\rangle_r;\ p_0 = 0;\ p_1 = p;\ p_i = \left\langle p_{i-1} + p \right\rangle_r,\ i = \overline{2, k-1}.$$

$$z = 1 + p \cdot k;\ z_0 = 0;\ z_1 = z;\ z_i = \left\langle z_{i-1} + z \right\rangle_N,\ i = \overline{2, k-1}. \quad (6)$$

Доказательство. Применяя рекуррентные соотношения к соотношениям (4) и (5), приходим к искомым формулам. С учетом леммы 2 табл. 1 может быть представлена в следующем виде.

Таблица 3 – Вычисление $S_r^i J_N$, $U^{p_i} S_r^i J_N$, $p_0 = z_0 = 0$, $p_i = \left\langle p_{i-1} + p \right\rangle_r$, $z_i = \left\langle z_{i-1} + z \right\rangle_N$, $i = \overline{1, k-1}$ для $N = k \cdot r = 3 \cdot 5 = 15$, где k, r – нечетные

i	$S_r^i J_N$	$p_i = \left\langle i \cdot p \right\rangle_r$	$U^{p_i} S_r^i J_N$	$z_i = \left\langle i \cdot z \right\rangle_N$
0	$S_5^0 J_{15} = (0, 3, 6, 9, 12)$	$p_0 = \left\langle 0 \cdot 3 \right\rangle_5 = 0$	$U^0 S_5^0 J_{15} = (0, 3, 6, 9, 12)$	$z_0 = \left\langle 0 \cdot 10 \right\rangle_{15} = 0$
1	$S_5^1 J_{15} = (1, 4, 7, 10, 13)$	$p_1 = \left\langle 1 \cdot 3 \right\rangle_5 = 3$	$U^3 S_5^1 J_{15} = (10, 13, 1, 4, 7)$	$z_1 = \left\langle 1 \cdot 10 \right\rangle = 10$
2	$S_5^2 J_{15} = (2, 5, 8, 11, 14)$	$p_2 = \left\langle 2 \cdot 3 \right\rangle_5 = 1$	$U^1 S_5^2 J_{15} = (5, 8, 11, 14, 2)$	$z_2 = \left\langle 2 \cdot 10 \right\rangle_{15} = 5$

Из табл. 3 видно, что секции можно строить сразу, опуская циклические сдвиги вверх. Для этого достаточно знать индекс первого элемента каждой секции. Индексы остальных элементов в каждой секции отличаются на шаг k, равный количеству секций при разбиении.

Рассмотрим построение секций, начиная с первых элементов секций, на примере последовательности $J_{28} = (0, 1, ..., 27)$. $N = 28$, $k = 4$, $r = 7$. Вычислим $p = d^{-1} = \left\langle (r-k)^{-1} \right\rangle_r = \left\langle 3^{-1} \right\rangle_7 = 5$, $d \cdot p - r \cdot r' = 3 \cdot 5 - 7 \cdot 2 = 1$, $z = 1 + p \cdot k = 1 + 5 \cdot 4 = 21$. Найдем z_i, $i = \overline{0, k-1} = \overline{0, 3}$, используя формулу (6).

Таблица 4 – Вычисление $S_r^i J_N$, $p_i = \left\langle i \cdot p \right\rangle_r$, $z_i = \left\langle i \cdot z \right\rangle_N$, $i = \overline{0, k-1}$, для $N = k \cdot r = 4 \cdot 7 = 28$, где k – четное, r – нечетное

i	$z_i = \left\langle i \cdot z \right\rangle_N$	$U^{p_i} S_r^i J_N$	$p_i = \left\langle i \cdot p \right\rangle_r$
$i = 0$	$z_0 = 0$	$U^0 S_7^0 J_{28} = (0, 4, 8, 12, 16, 20, 24)$	$p_0 = \left\langle 0 \cdot 5 \right\rangle_7 = 0$
$i = 1$	$z_i = z = 21$	$U^5 S_7^1 J_{28} = (21, 25, 1, 5, 9, 13, 17)$	$p_1 = \left\langle 1 \cdot 5 \right\rangle_7 = 5$
$i = 2$	$z_2 = \left\langle 2 \cdot 21 \right\rangle_{28} = 14$	$U^3 S_7^2 J_{28} = (14, 18, 22, 26, 2, 6, 10)$	$p_2 = \left\langle 2 \cdot 5 \right\rangle_7 = 3$
$i = 3$	$z_3 = \left\langle 3 \cdot 21 \right\rangle_{28} = 7$	$U^1 S_7^3 J_{28} = (7, 11, 15, 19, 22, 27, 3)$	$p_3 = \left\langle 3 \cdot 5 \right\rangle_7 = 1$

Таблица 5 – Вычисление секций для $N = k \cdot r = 9 \cdot 11 = 99$, где k, r – нечетные, $p = 6$, $z = 55$

i	$z_i = \left\langle i \cdot z \right\rangle_{99}$	i	$z_i = \left\langle i \cdot z \right\rangle_{99}$	i	$z_i = \left\langle i \cdot z \right\rangle_{99}$
0	$z_0 = 0$	3	$z_3 = 66$	6	$z_6 = 33$
1	$z_1 = 55$	4	$z_4 = 22$	7	$z_7 = 88$
2	$z_2 = 11$	5	$z_5 = 77$	8	$z_8 = 44$

Лемма 3. Пусть последовательность $J_N = (0, 1, ..., N-1)$, $N = k \cdot r$, $(k, r) = 1$, $k < r$ упорядочена: $P_r^i(T_N) = U^{p_i}(S_r^i(J_N))$, $p_i = \left\langle i \cdot p \right\rangle_r$, $i = \overline{0, k-1}$, где $p = \left\langle (r-k)^{-1} \right\rangle_r$. Тогда к первоначальному порядку полученную последовательность T_N переводят следующие соотношения:

$$p = \left\langle (r-k)^{-1} \right\rangle_r;\ P_r^i(T_N) = D^{p_i}(P_r^i(T_N)),\ p_i = \left\langle i \cdot p \right\rangle_r,\ i = \overline{0, k-1}.$$

$$P_k^i(J_N) = S_k^i(T_N),\ i = \overline{0, r-1}, \tag{7}$$

Доказательство. Оператор U^{p_i} (*up*-вверх) в выражении $U^{p_i} S_r^i J_N$ циклически сдвигает вверх каждую секцию i на p_i раз. Соответственно, чтобы получить значения секции в первоначальном (исходном) состоянии, нужно применить обратный оператор D (*down*-вниз) для каждой секции p_i раз, т.е. циклически сдвинуть вниз каждую секцию i на такое же p_i раз: $P_r^i T_N = D^{p_i}(P_r^i T_N)$, $i = \overline{0, k-1}$. После этого первоначальными элементами каждой секции i будут элементы со значениями i, которые отстоят друг от друга на r элементов (длина каждой секции равна r). Получили следующую последовательность, состоящую из секций, выделенных вертикальными линиями:

$$0, k, ..., (r-1) \cdot k \mid 1, 1+k, ..., 1+(r-1) \cdot k \mid ... \mid k-1, 2k-1, ..., N-1.$$

Выборка первых элементов, отстоящих друг от друга на r шагов, из k секций определяется выражением $S_k^0 T_N$, что соответствует последовательности $(0, 1, ..., k-1)$. Выборка элементов $(k, k+1, ..., 2k-1)$, следующими за первыми в каждой секции, определяется выражением $S_k^1 T_N$. Продолжая выборку по формуле (7), получим первоначальную последовательность.

Лемма доказана.

Более детально рассмотрим последовательность J_{15} длиной 15 элементов $k=3$, $r=5$. Согласно табл. 3 упорядочивание $P_5^i J_{15} = U^{p_i} S_5^i J_{15}$, $p_i = \langle i \cdot 3 \rangle_r$, $i = \overline{0, 2}$, дает следующую последовательность, разбитую на 3 секции:

$$T_{15} = (0, 3, 6, 9, 12 \mid 10, 13, 1, 4, 7 \mid 5, 8, 11, 14, 2).$$

Выражения $P_5^i T_{15} = D^{p_i}(P_5^i J_{15})$, $p_i = \langle i \cdot 3 \rangle_5$, $i = \overline{0,2}$, приводят предыдущую последовательность к следующему виду:

$$T_{15} = (0, 3, 6, 9, 12 \mid 1, 4, 7, 10, 13 \mid 2, 5, 8, 11, 14).$$

Соотношения $P_3^i J_{15} = S_3^i T_{15}$, $i = \overline{0, 4}$, приводят к первоначальной последовательности:

$$J_{15} = (0, 1, 2 \mid 3, 4, 5 \mid 6, 7, 8 \mid 9, 10, 11 \mid 12, 13, 14).$$

Лемма 4. Циклическую свертку R_N длины $N = k \cdot r$, $k = r-1$, $(k, r) = 1$ сигналов X_N и Y_N выражения $P_i X_N = U^i S_r^i X_N$, $P_i Y_N = U^i S_r^i Y_N$, $P_i R_N = U^i S_r^i R_N$, $i = \overline{0, k-1}$ переводят в блочно-циклический вид.

Доказательство. Циклическая свертка сигналов X_N и Y_N определяется выражением $r_j = \sum_{m=0}^{N-1} x_{\langle m-j \rangle_N} \cdot y_m$, $j = \overline{0, N-1}$.

Воспользуемся оператором S и найдем секции длиной r для сигнала X_N (преобразования для сигнала Y_N не приводятся, т.к. они аналогичны):

$$S_r^0 X_N = \begin{bmatrix} x_0 \\ x_k \\ \dots \\ x_{N-2k} \\ x_{N-k} \end{bmatrix}, \; S_r^1 X_N = \begin{bmatrix} x_1 \\ x_{k+1} \\ \dots \\ x_{N-2k+1} \\ x_{N-k+1} \end{bmatrix}, \; \dots, \; S_r^{k-1} X_N = \begin{bmatrix} x_{k-1} \\ x_{2k-1} \\ \dots \\ x_{N-k-1} \\ x_{N-1} \end{bmatrix}. \qquad (8)$$

Элементы каждой секции i, полученные с использованием оператора S, сдвинем циклически вверх на i раз $i = \overline{0, k-1}$:

$$U^0 S_r^0 X_N = \begin{bmatrix} x_0 \\ x_k \\ \dots \\ x_{N-2k} \\ x_{N-k} \end{bmatrix}, \; U^1 S_r^1 X_N = U^1 \begin{bmatrix} x_1 \\ x_{1+k} \\ \dots \\ x_{1+N-2k} \\ x_{1+N-k} \end{bmatrix} = U^1 \begin{bmatrix} x_1 \\ x_r \\ \dots \\ x_{1+N-2k} \\ x_{1+N-k} \end{bmatrix} = \begin{bmatrix} x_r \\ x_{r+k} \\ \dots \\ x_{1+N-k} \\ x_1 \end{bmatrix},$$

$$U^2 S_r^2 X_N = U^2 \begin{bmatrix} x_2 \\ x_{2+k} \\ x_{2+2k} \\ \dots \\ x_{2+N-k} \end{bmatrix} = U^2 \begin{bmatrix} x_2 \\ x_{2+k} \\ x_{2r} \\ \dots \\ x_{2+N-k} \end{bmatrix} = \begin{bmatrix} x_{2r} \\ x_{2r+k} \\ x_{2r+2k} \\ \dots \\ x_{2+k} \end{bmatrix}, \ \dots, \qquad (9)$$

$$U^i S_r^i X_N = \begin{bmatrix} x_{i\cdot r} \\ x_{i\cdot r+k} \\ \dots \\ x_{i\cdot r-2k} \\ x_{i\cdot r-k} \end{bmatrix}, \ \dots, \ U^{k-1} S_r^{k-1} X_N = \begin{bmatrix} x_{(k-1)\cdot r} \\ x_{(k-1)\cdot r+k} \\ \dots \\ x_{(k-1)\cdot r-2k} \\ x_{(k-1)\cdot r-k} \end{bmatrix} = \begin{bmatrix} x_{N-r} \\ x_{N-r+k} \\ \dots \\ x_{N-r-2k} \\ x_{N-r-k} \end{bmatrix}.$$

Из (9) видно, что индексы при x первых (самых верхних) элементах каждой секции делятся на r:

$$[U^i S_r^i X_N]_0 = x_{i\cdot r}, \ i = \overline{0, k-1}.$$

Так как каждая секция построена таким образом, что индекс при x следующего элемента в секции отличается от предыдущего на k, то все элементы секций можно записать следующим образом:

$$[U^i S_r^i X_N]_j = x_{<z_i + j\cdot k>_N}, \ j = \overline{0, r-1}, \ z_i = i \cdot r, \ i = \overline{0, k-1}. \qquad (10)$$

Вычисление свертки с учетом (10) можно представить в следующем виде

$$r_{\langle q\cdot r + m\cdot k\rangle_N} = \sum_{i=0}^{k-1}\sum_{j=0}^{r-1} x_{\langle (i\cdot r - q\cdot r) + (j\cdot k - m\cdot k)\rangle_N} \cdot y_{\langle i\cdot r + j\cdot k\rangle_N}, \ m = \overline{0, r-1}, \ q = \overline{0, k-1}. \qquad (11)$$

Из данного соотношения видно, что в каждой колонке $\langle q\cdot r + m\cdot k\rangle_N$ матрицы (рис. 2) индексы при x и y каждой строчки $\langle i\cdot r + j\cdot k\rangle_N$ отличаются на одно и то же число $\langle -q\cdot r - m\cdot k\rangle_N$, что говорит о свойстве цикличности данного представления.

Рассмотрим вычисление свертки.

$$\begin{array}{c|c:c:c:c}
\begin{bmatrix} y_0 \\ y_k \\ \\ y_{N-k} \end{bmatrix} & \begin{bmatrix} x_0 & x_{N-k} & \dots & x_k \\ x_k & x_0 & \dots & x_{2k} \\ \dots & \dots & \dots & \dots \\ x_{N-k} & x_{N-2k} & \dots & x_0 \end{bmatrix} & \begin{bmatrix} x_{N-r} & x_{N-r-k} & \dots & x_{N-1} \\ x_{N-r+k} & x_{N-r} & \dots & x_{k-1} \\ \dots & \dots & \dots & \dots \\ x_{N-r-k} & x_{N-r-2k} & \dots & x_{N-r} \end{bmatrix} & \dots & \begin{bmatrix} x_r & x_1 & \dots & x_{r+k} \\ x_{r+k} & x_r & \dots & x_{r+2k} \\ \dots & \dots & \dots & \dots \\ x_1 & x_{N-k+1} & \dots & x_r \end{bmatrix} \\ \hdashline
\begin{bmatrix} y_r \\ y_{r+k} \\ \\ y_1 \end{bmatrix} & \begin{bmatrix} x_r & x_1 & \dots & x_{r+k} \\ x_{r+k} & x_r & \dots & x_{r+2k} \\ \dots & \dots & \dots & \dots \\ x_1 & x_{N-k+1} & \dots & x_r \end{bmatrix} & \begin{bmatrix} x_0 & x_{N-k} & \dots & x_k \\ x_k & x_0 & \dots & x_{2k} \\ \dots & \dots & \dots & \dots \\ x_{N-k} & x_{N-2k} & \dots & x_0 \end{bmatrix} & \dots & \begin{bmatrix} x_{2r} & x_{2r-k} & \dots & x_{2r+k} \\ x_{2r+k} & x_{2r} & \dots & x_{2r+2k} \\ \dots & \dots & \dots & \dots \\ x_{2r-k} & x_{2r-2k} & \dots & x_{2r} \end{bmatrix} \\ \hdashline
\dots & \dots & \dots & \dots & \dots \\ \hdashline
\begin{bmatrix} y_{N-r} \\ y_{N-r+k} \\ \\ y_{N-r-k} \end{bmatrix} & \begin{bmatrix} x_{N-r} & x_{N-r-k} & \dots & x_{N-r+k} \\ x_{N-r+k} & x_{N-r} & \dots & x_{-r+2k} \\ \dots & \dots & \dots & \dots \\ x_{N-r-k} & x_{N-r-2k} & \dots & x_{N-r} \end{bmatrix} & \begin{bmatrix} x_{N-2r} & x_{N-2r-k} & \dots & x_{N-2r+k} \\ x_{N-2r+k} & x_{N-2r} & \dots & x_{N-2r+2k} \\ \dots & \dots & \dots & \dots \\ x_{N-2r-k} & x_{N-2r-2k} & \dots & x_{N-2r} \end{bmatrix} & \dots & \begin{bmatrix} x_0 & x_{N-k} & \dots & x_k \\ x_k & x_0 & \dots & x_{2k} \\ \dots & \dots & \dots & \dots \\ x_{N-k} & x_{N-2k} & \dots & x_0 \end{bmatrix} \\ \hline
 & \begin{bmatrix} r_0 & r_k & \dots & r_{N-k} \end{bmatrix} & \begin{bmatrix} r_r & r_{r+k} & \dots & r_1 \end{bmatrix} & \dots & \begin{bmatrix} r_{N-r} & r_{N-r+k} & \dots & r_{N-r-k} \end{bmatrix}
\end{array}$$

Рисунок 2 – Вычисление свертки длины $N = k\cdot r$, $r = k+1$

Для доказательства блочности представления достаточно исследовать верхние левые элементы секций (блоков). С учетом соотношения (11) (при $m=0$, $j=0$) получаем следующие выражения:

$$x_{\langle i\cdot r-q\cdot r\rangle_N}\cdot y_{\langle i\cdot r\rangle},\ i=\overline{0,k-1},\ q=\overline{0,k-1}, \qquad (12)$$

где $x_{\langle i\cdot r-q\cdot r\rangle_N}\cdot y_{\langle i\cdot r\rangle}$ элемент строчки $\langle i\cdot r\rangle_N$ и столбцы $\langle -q\cdot r\rangle_N$ матрицы.

Откуда видно, что угловые элементы $x_{\langle (i-q)\cdot r\rangle_N}$, $i=\overline{0,k-1}$, $q=\overline{0,k-1}$, отстоят друг от друга на r строчек и столбцов. Выражение $\langle (i-q)\cdot r\rangle_N = r\cdot\langle i-q\rangle_k$, $i=\overline{0,k-1}$, $q=\overline{0,k-1}$ показывает, что элемент x с одним и тем же индексом $r\cdot\langle i-q\rangle_k$ в верхних левых углах блоков повторяется k раз.

Для демонстрации шага индекса между секциями, шага индекса внутри секции и корректности построения свертки достаточно использовать более компактное представление:

$$\begin{array}{c|c:c:c}
\begin{bmatrix} y_0 \\ y_k \\ \ldots \end{bmatrix} & \begin{bmatrix} x_0 & x_{N-k} & \ldots \\ x_k & x_0 & \ldots \\ \ldots & \ldots & \ldots \end{bmatrix} & \begin{bmatrix} x_{N-r} & x_{N-r-k} & \ldots \\ x_{N-r+k} & x_{N-r} & \ldots \\ \ldots & \ldots & \ldots \end{bmatrix} & \ldots \\ \hdashline
\begin{bmatrix} y_r \\ y_{r+k} \\ \ldots \end{bmatrix} & \begin{bmatrix} x_r & x_1 & \ldots \\ x_{r+k} & x_r & \ldots \\ \ldots & \ldots & \ldots \end{bmatrix} & \begin{bmatrix} x_0 & x_{N-k} & \ldots \\ x_k & x_0 & \ldots \\ \ldots & \ldots & \ldots \end{bmatrix} & \ldots \\ \hdashline
\ldots & \ldots & \ldots & \ldots \\ \hline
 & \begin{bmatrix} r_0 & r_k & \ldots \end{bmatrix} & \begin{bmatrix} r_r & r_{r+k} & \ldots \end{bmatrix} & \ldots
\end{array}$$

Рисунок 3 – Индексы в секции и между секциями

Из рис. 3 несложно определить количество элементов в каждой секции и число секций, необходимых для построения свертки. Из рис. 3 также видно, что с учетом того, что шаг индекса внутри каждой секции равен k и шаг индекса между секциями делится на r, где $r=k+1$, свертка построена корректно.

С учетом (12) и операторов U и S вычисление свертки $N=k\cdot r$, $r=k+1$, можно представить следующим образом:

$U^0S_r^0Y_N$	$U^0S_r^0X_N$	$U^{k-1}S_r^{k-1}X_N$	...	$U^1S_r^1X_N$
$U^1S_r^1Y_N$	$U^1S_r^1X_N$	$U^0S_r^0X_N$	...	$U^2S_r^2X_N$
...	...	...	...	...
$U^{k-1}S_r^{k-1}Y_N$	$U^{k-1}S_r^{k-1}X_N$	$U^{k-2}S_r^{k-2}X_N$	...	$U^0S_r^0X_N$
	$U^0S_r^0R_N$	$U^1S_r^1R_N$	...	$U^{k-1}S_r^{k-1}R_N$

Рисунок 4 – Вычисление свертки длины $N=k\cdot r$, $r=k+1$ в операторном виде

С учетом обозначений $X_N^i=U^iS_r^iX_N$, $Y_N^i=U^iS_r^iY_N$, $R_N^i=U^iS_r^iR_N$ рис. 4 можно представить в блочном виде, в котором вычисление свертки длины $N=k\cdot r$, $(k,r)=1$, $r-k=1$, сводится к вычислению k сверток длины r.

Лемма доказана.

Y_N^0	X_N^0	X_N^{k-1}	...	X_N^1
Y_N^1	X_N^1	X_N^0	...	X_N^0
...	...	...	...	...
Y_N^{k-1}	X_N^{k-1}	X_N^{k-2}	...	X_N^0
	R_N^0	R_N^1	...	R_N^{k-1}

Рисунок 5 – Свертка длины $N = k \cdot r$, $r = k + 1$ в блочном виде

Продемонстрируем вычисление свертки при k – нечетном, $r = k + 1$ и покажем на примере вычисления свертки длины $N = 12 = 3 \cdot 4$. Вычисление можно представить в виде:

$U^0 S_4^0 Y_{12}$	y_0	x_0	x_9	x_6	x_3	x_8	x_5	x_2	x_{11}	x_4	x_1	x_{10}	x_7
	y_3	x_3	x_0	x_9	x_6	x_{11}	x_8	x_5	x_2	x_7	x_4	x_1	x_{10}
	y_6	x_6	x_3	x_0	x_9	x_2	x_{11}	x_8	x_5	x_{10}	x_7	x_4	x_1
	y_9	x_9	x_6	x_3	x_0	x_5	x_2	x_{11}	x_8	x_1	x_{10}	x_6	x_4
$U^1 S_4^1 Y_{12}$	y_4	x_4	x_1	x_{10}	x_7	x_0	x_9	x_6	x_3	x_8	x_5	x_2	x_{11}
	y_7	x_7	x_4	x_1	x_{10}	x_3	x_0	x_9	x_6	x_{11}	x_8	x_5	x_2
	y_{10}	x_{10}	x_7	x_4	x_1	x_6	x_3	x_0	x_9	x_2	x_{11}	x_8	x_5
	y_1	x_1	x_{10}	x_6	x_4	x_9	x_6	x_3	x_0	x_5	x_2	x_{11}	x_8
$U^2 S_4^2 Y_{12}$	y_8	x_8	x_5	x_2	x_{11}	x_4	x_1	x_{10}	x_7	x_0	x_9	x_6	x_3
	y_{11}	x_{11}	x_8	x_5	x_2	x_7	x_4	x_1	x_{10}	x_3	x_0	x_9	x_6
	y_2	x_2	x_{11}	x_8	x_5	x_{10}	x_7	x_4	x_1	x_6	x_3	x_0	x_9
	y_5	x_5	x_2	x_{11}	x_8	x_1	x_{10}	x_6	x_4	x_9	x_6	x_3	x_0
		r_0	r_3	r_6	r_9	r_4	r_7	r_{10}	r_1	r_8	r_{11}	r_2	r_5
		$U^0 S_4^0 R_{12}$				$U^1 S_4^1 R_{12}$				$U^2 S_4^2 R_{12}$			

Рисунок 6 – Вычисления свертки длины $N = 3 \cdot 4$

$U^0 S_4^0 Y_{12}$	$U^0 S_4^0 X_{12}$	$U^2 S_4^2 X_{12}$	$U^1 S_4^1 X_{12}$
$U^1 S_4^1 Y_{12}$	$U^1 S_4^1 X_{12}$	$U^0 S_4^0 X_{12}$	$U^2 S_4^2 X_{12}$
$U^2 S_4^2 Y_{12}$	$U^2 S_4^2 X_{12}$	$U^1 S_4^1 X_{12}$	$U^0 S_4^0 X_{12}$
	$U^0 S_4^0 R_{12}$	$U^1 S_4^1 R_{12}$	$U^2 S_4^2 R_{12}$

Рисунок 7 – Вычисление свертки длины $N = 3 \cdot 4$ в операторном виде

Индексы в операторах S, U для входных и выходного сигналов совпадают в соответствующих секциях.

С учетом того, что для вычисления свертки длины $N = 3$ и $N = 4$ необходимо 4 и 5 операций умножения соответственно [6], для вычисления свертки длины $N = 12 = 3 \cdot 4$ необходимо 20 операций умножения, что соответствует оценке Винограда [8]. Это на 4 операции меньше, чем разбиение $N = 12 = 2 \cdot 6 = 2 \cdot (2 \cdot 3)$ на две секции по 6 элементов, которые разбиваются далее на 2 секции по 3 элемента (для вычисления свертки таким способ необходимо 24 операции однословного умножения [4]).

Лемма 5. Циклическую свертку R_N длины $N = k \cdot r$, $r - k = d \geq 1$, $(k, r) = 1$ сигналов X_N и Y_N соотношения $\langle p \cdot d \rangle_r = 1$; $P_i X_N = U^{p_i} S_r^i X_N$, $P_i Y_N = U^{p_i} S_r^i Y_N$, $P_i R_N = U^{p_i} S_r^i R_N$, $p_i = \langle p \cdot i \rangle_r$, $i = \overline{0, k-1}$ переводят к блочно-циклическому виду.

Доказательство. Воспользуемся оператором S (8) и найдем секции длиной r входных X_N, Y_N и выходного R_N сигналов. С учетом леммы 2 элементы каждой секции сдвинем циклически вверх p_i раз, $i = \overline{0, k-1}$.

$$z = 1 + p \cdot k, \; p = d^{-1} = \left\langle (r-k)^{-1} \right\rangle_r; \; p_i = \langle i \cdot p \rangle_r, \; z_i = \langle z \cdot i \rangle_N, \; i = \overline{0, k-1};$$

$$U^0 S_r^0 X_N = \begin{bmatrix} x_0 \\ x_k \\ \ldots \\ x_{N-2k} \\ x_{N-k} \end{bmatrix}, \ldots, U^{p_i} S_r^i X_N = \begin{bmatrix} x_{z_i} \\ x_{z_i+k} \\ \ldots \\ x_{z_i-2k} \\ x_{z_i-k} \end{bmatrix}, \ldots, U^{p_{k-1}} S_r^{k-1} X_N = \begin{bmatrix} x_{z_{k-1}} \\ x_{z_{k-1}+k} \\ \ldots \\ x_{z_{k-1}-2k} \\ x_{z_{k-1}-k} \end{bmatrix}. \quad (13)$$

С учетом (13) вычисление свертки можно представить в виде:

$U^0 S_r^0 Y_N$	$U^0 S_r^0 X_N$	$U^{p_{k-1}} S_r^{k-1} X_N$	...	$U^{p_1} S_r^1 X_N$
$U^{p_1} S_r^1 Y_N$	$U^{p_1} S_r^1 X_N$	$U^0 S_r^0 X_N$	...	$U^{p_2} S_r^2 X_N$
...	...	...	...	...
$U^{p_{k-1}} S_r^{k-1} Y_N$	$U^{p_{k-1}} S_r^{k-1} X_N$	$U^{p_{k-2}} S_r^{k-2} X_N$	...	$U^0 S_r^0 X_N$
	$U^0 S_r^0 R_N$	$U^{p_1} S_r^1 R_N$	...	$U^{p_{k-1}} S_r^{k-1} R_N$

Рисунок 8 – Вычисление свертки с использованием операторов U и S

Вычисление свертки можно представить в виде следующих выражений:

$$p = \left\langle (r-k)^{-1} \right\rangle_r, \; z = 1 + p \cdot k; \; r_{\langle q \cdot r + m \cdot k \rangle_N} = \sum_{i=0}^{k-1} t_i, \; t_i = \sum_{j=0}^{r-1} x_{\langle (z_i - q \cdot r) + (j \cdot k - m \cdot k) \rangle_N} \cdot y_{\langle z_i + j \cdot k \rangle_N},$$

$$z_i = \langle z \cdot i \rangle_N,$$

$$i = \overline{0, k-1}, \; m = \overline{0, r-1}, \; q = \overline{0, k-1}. \quad (14)$$

Из (14) видно, что в каждой колонке $\langle q \cdot r + m \cdot k \rangle_N$ свертки индексы при x и y в каждой строчке $\langle z_i + j \cdot k \rangle_N$ отличаются на одно и то же число $\langle -q \cdot r - m \cdot k \rangle_N$, что говорит о свойстве цикличности данного представления.

С учетом обозначений $X_N^i = U^{p_i} S_r^i X_N$, $Y_N^i = U^{p_i} S_r^i Y_N$, $R_N^i = U^{p_i} S_r^i R_N$ рис. 8 можно представить в блочном виде, аналогичном рис. 5.

Лемма доказана.

Лемма 4 является частным случаем леммы 5 и (14) равнозначна (12) при $r - k = d = 1$ ($p = \langle d^{-1} \rangle_r = \left\langle (r-k)^{-1} \right\rangle_r = 1$, $z = r$).

Априорные оценки сложности

Теорема 1. Априорная оценка сложности вычисления циклической свертки длины $N = k \cdot r$, $(k,r)=1$, $r-k=d \geq 1$, где k и r – взаимно простые числа, имеет вид:

$$Q^*(N) \leq Q^*(k) \cdot Q^*(r)\,,\ Q^{\pm}(N) \leq Q^{\pm}(k) \cdot r + Q^*(k) \cdot Q^{\pm}(r)\,, \tag{15}$$

где $Q^*(k)$, $Q^*(r)$, $Q^{\pm}(k)$, $Q^{\pm}(r)$ – количество операций умножения, сложения и вычитания для вычисления циклических сверток длины k и r.

Доказательство. Циклическая свертка сигналов X_N и Y_N, где $N = k \cdot r$, $(k,r)=1$, $r-k=d \geq 1$, может быть представлена в блочно-циклическом виде (рис. 5, 8). Если $Q^*(k)$, $Q^*(r)$, $Q^{\pm}(k)$, $Q^{\pm}(r)$ – количество операций умножения, сложения и вычитания, необходимых для вычисления циклических сверток длины k и r, то общую сложность вычисления свертки длины $N = k \cdot r$ можно представить априорными оценками (15).

Теорема доказана.

Теорема 1 применима в следующих случаях:

1. k – нечетное, r – четное, $k < r$.
2. k – нечетное, r – нечетное, $k < r$, k и r – взаимно простые.
3. k – четное, r – нечетное, $k < r$.

Случай, когда k, r – четные, не рассматривается, так как по условию числа k и r взаимно простые. Вычисление свертки вида $N = 2 \cdot k$, k – нечетное [4], является частным случаем теоремы 1.

Теорема 2. Априорная оценка сложности вычисления циклической свертки длины $N = \prod_{i=0}^{n-1} m_i$, $(m_i, m_j) = 1$, $i \neq j$, $m_0 < m_1 < ... < m_{n-2} < m_{n-1}$, имеет вид:

$$Q^*(N) \leq \prod_{i=0}^{n-1} Q^*(m_i)\,,\ Q^{\pm}(N) \leq \sum_{i=0}^{n-1} \left(\left(\prod_{k=0}^{i-1} Q^*(m_i) \right) \cdot Q^{\pm}(m_i) \cdot \left(\prod_{k=i+1}^{n-1} m_k \right) \right),$$

где $Q^*(m_i)$, $Q^{\pm}(m_i)$ – количество операций умножения, сложения и вычитания, необходимых для вычисления циклической свертки длины m_i.

Доказательство. Рассмотрим свертку длины $N = m_0 \cdot N_0$, где $(m_0, N_0) = 1$ взаимно простые, тогда согласно теореме 1 априорные оценки сложности можно выразить следующими выражениями:

$$Q^*(N) \leq Q^*(m_0) \cdot Q^*(N_0)\,,\ Q^{\pm}(N) \leq Q^{\pm}(m_0) \cdot N_0 + Q^*(m_0) \cdot Q^{\pm}(N_0)\,, \tag{16}$$

где $Q^*(m_0)$, $Q^{\pm}(m_0)$, $Q^*(N_0)$, $Q^{\pm}(N_0)$ – количество операций умножения, сложения и вычитания, необходимых для вычисления циклических сверток длины m_0 и N_0.

Пусть $N_0 = m_1 \cdot N_1$ также является произведением взаимно простых чисел $(m_1, N_1) = 1$, тогда согласно теореме 1 и формуле (16) априорные оценки сложности для свертки длины $N = m_0 \cdot N_0 = m_0 \cdot m_1 \cdot N_1$ можно выразить следующими выражениями:

$$Q^*(N) \le Q^*(m_0)\cdot Q^*(N_0) = Q^*(m_0)\cdot\left(Q^*(m_1)\cdot Q^*(N_1)\right),$$

$$Q^{\pm}(N) \le Q^{\pm}(m_0)\cdot N_0 + Q^*(m_0)\cdot Q^{\pm}(N_0)$$

$$Q^{\pm}(N) \le Q^{\pm}(m_0)\cdot m_1\cdot N_1 + Q^*(m_0)\cdot\left(Q^{\pm}(m_1)\cdot N_1 + Q^*(m_1)\cdot Q^{\pm}(N_1)\right)$$

$$Q^{\pm}(N) \le Q^{\pm}(m_0)\cdot m_1\cdot N_1 + Q^*(m_0)\cdot Q^{\pm}(m_1)\cdot N_1 + Q^*(m_0)\cdot Q^*(m_1)\cdot Q^{\pm}(N_1),$$

где $Q^*(m_0)$, $Q^{\pm}(m_0)$, $Q^*(m_1)$, $Q^{\pm}(m_1)$, $Q^*(N_1)$, $Q^{\pm}(N_1)$ – количество операций умножения, сложения и вычитания, необходимых для вычисления циклических сверток длины m_0, m_1 и N_1. Продолжая разбиение N_1 на меньшие длины, приходим к соотношениям (16).

Теорема доказана.

Оценки в теоремах 1 и 2 аналогичны оценкам, полученным Р.К. Агарвалом и Дж.У. Кули при реализации метода с использованием китайской теоремы об остатках [9, с. 104-105].

Следствие 1. Если сомножители являются степенью числа: $N = \prod_{i=0}^{k-1} m_i^{n_i}$, то деление на меньшие свертки должно производиться в порядке возрастания величины сомножителей $m_0^{n_0} < m_1^{n_1} < \ldots < m_{k-2}^{n_{k-2}} < m_{k-1}^{n_{k-1}}$, а не в порядке возрастания основания числа $m_0 < m_1 < \ldots < m_{k-2} < m_{k-1}$. Так разбиение свертки длины $2^5\cdot 3^4\cdot 5^2\cdot 7^2$ производится следующим образом: $5^2 < 2^5 < 7^2 < 3^4$ ($25 < 32 < 49 < 81$). Сначала каждый сигнал разбивается на 25 секций, каждая из которых разбивается на 32 секции и т.д.

Следствие 2. При группировке сомножителей порядок разбиения меняется.

Имеется в виду, что число сомножителей может быть уменьшено за счет группировки сомножителей. Так, в предыдущем примере при группировке сомножителей 25 и 49 меняется порядок разбиения $32 < 81 < 25\cdot 49$. Это свойство является очень важным, так как для одной и той же длины свертки возможны различные разбиения с различной оценкой сложности, среди которых можно выделить лучшую оценку. Важным является то, что возможно комбинирование методов. Так, например, в предыдущем примере $32 < 81 < 25\cdot 49$ первый сомножитель является степенью двойки, что позволяет использовать методы, основанные на представлении большей свертки за счет нескольких сверток половинной длины. Для остальных шагов $\ldots < 81 < 25\cdot 49$ будут использоваться другие методы. Если в начале последовательности $2 < 3 < 5 < 7 < \ldots$ стоят маленькие числа, то актуальным встает вопрос оптимизации вычислений не только длинных, но и коротких сверток.

Таблица 6 – Количество операций умножения для вычисления коротких сверток [6, с. 67-70]

N	2	3	4	5	7	8	9
$Q^*(N)$	2	4	5	10	16	14	19

Далее в таблицах приведены априорные оценки сложности по количеству операций однословного умножения для вычисления циклической свертки различной длины разными методами.

Таблица 7 – Количество операций умножения для вычисления сверток длиной, равной произведению взаимно простых чисел предложенным методом

$N=\prod_{i=0}^{n-1} m_i$	6=2·3	10=2·5	18=2·9	24=3·8	35=5·7	63=7·9
$Q^*(N)=\prod_{i=0}^{n-1} Q_i^*(m_i)$	8=2·4	20=2·10	38=2·19	42=3·14	160=10·16	304=16·19

Таблица 8 – Количество операций умножения для вычисления сверток с использованием преобразования Уолша [3]

n	3	4	5	6
$N=2^n$	8	16	32	64
$Q^*(N)=5\cdot 3^{n-2}$	15	45	135	405

С учетом того, что при умножении двух N разрядных чисел получается $2N$ разрядное число, можно использовать свертку длины 63 для умножения чисел длиной 32 слова. Согласно табл. 7 необходимо 304 целочисленных операций однословного умножения для реализации операции 32 разрядного умножения. Для сравнения: для вычисления дискретного преобразования Фурье длины 64 для одного числа необходимо $(64/2)\cdot\log_2 64=192$ операции, где присутствуют операции с плавающей запятой, а для реализации операции умножения, основанной на преобразовании Фурье необходимо выполнять прямое и обратное преобразования.

Метод удобен также тем, что пред- и поствычисления в виде циклических сдвигов для обоих входных сигналов одинаковые, что является отличием от методов Агарвала – Кули и Агарвала – Барраса.

Выводы

В данной работе предложен метод вычисления сверток длины, равной произведению взаимно простых чисел с использованием циклических сдвигов и без использования китайской теоремы об остатках. Предложенный метод позволяет параллельно вычислять свертки меньшей размерности. Приведены априорные оценки сложности вычисления сверток длиной, равной произведению двух и более взаимно простых сомножителей. Приведены зависимости между элементами секций, числом секций, длиной секций, на которые разбиваются свертки. Приведены примеры разбиения циклических сверток разных длин. Предложенный метод может быть использован для вычисления циклической свертки целочисленных, вещественных или комплексных сигналов.

Литература

1. Залманзон Л.А. Преобразование Фурье, Уолша, Хаара и их применение в управлении, связи и других областях / Залманзон Л.А. – М. : Наука, 1989. – 496 с.
2. Pitassi D.A. Fast convolution using the Walsh transform / D.A. Pitassi // Applicat. Walsh Functions. – 1971. – April. – P. 130-133.
3. Davis W.F. A class of efficient convolution algorithms / W.F. Davis // Applicat. Walsh Functions. – 1972. – March. – P. 318-329.

4. Терещенко А.Н. Оптимизация метода Питасси вычисления свертки / А.Н. Терещенко // Искусственный интеллект. – 2009. – № 1 – С. 204-212.
5. Реализация операции умножения с использованием преобразования Уолша / А.Н. Терещенко, С.С. Мельникова, Л.А. Гнатив [и др.] // Проблемы управления и информатики. – 2010. – № 2. – С. 102-126.
6. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток / Нуссбаумер Г. ; пер. с англ. – М. : Радио и связь, 1985.
7. Agarwal R.C. Fast one-dimensional digital convolution by multidimensional technique / R.C. Agarwal ad C.S. Burrus // IEEE Trans, Acoust., Speech, Signal Processing. – 1974. – Feb. – Vol. ASSP-22. – P. 1-10.
8. Winograd S. Some bilinear forms whose multiplicative complexity depends on the field of constants / S. Winograd // Mathematical Systems Theory. – Vol. 10.
9. Макклеллан Дж.Г. Применение теории чисел в цифровой обработке сигналов / Дж.Г. Макклеллан, Ч.М. Райдер ; пер. с англ. / под ред. Ю.И. Манина. – М. : Радио и связь, 1983. – 264 с., ил.
10. Задирака В.К. Построение программно-аппаратных комплексов арифметики сверхбольших чисел / В.К. Задирака, А.М. Кудин // Комп'ютерна математика. Оптімізація обчислень : збірник наукових праць НАНУ, Ін-т кібернетики ім. В.М. Глушкова. – Київ, 2001. – Т. 1. – С. 158-163.

Literatura

1. Zalmanzon L.A. Preobrazovanie Fur'e, Uolsha, Haara i ih primenenie v upravlenii, svjazi i drugih oblastjah. M.: Nauka. 1989. 496 s.
2. Pitassi D.A. Applicat. Walsh Functions. April 1971. P. 130-133.
3. Davis W.F Applicat. Walsh Functions. March 1972. P. 318-329.
4. Tereshhenko A.N. Iskusstvennyj intellekt. № 1. 2009. S. 204-212.
5. Tereshhenko A.N. Mezhdunarodnyj nauchno-tehnicheskij zhurnal Problemy upravlenija i informatiki. № 2. 2010. S. 102-126.
6. Nussbaumer G. Bystroe preobrazovanie Fur'e i algoritmy vychislenija svertok. M. : Radio i svjaz'. 1985. 66 s.
7. R.C. Agarwal. IEEE Trans, Acoust., Speech, Signal Processing. Feb. 1974. Vol. ASSP-22. P. 1-10.
8. Winograd S. Mathematical Systems Theory. Vol 10.
9. Makklellan Dzh.G. Primenenie teorii chisel v cifrovoj obrabotke signalov. M.: Radio i svjaz'. 1983. 264 s.
10. Zadiraka V.K. Komp'juternaja matematika. Optimizacija obchislen': Zbirnik naukovih prac' NANU, Int-t kibernetiki im. V.M. Glushkova. Kyiv. T. 1. 2001. S. 158-163.

А.М. Терещенко, В.К. Задірака, А.М. Кудін

Використання циклічних зсувів для прискореного обчислення циклічних згорток довжини, яка дорівнює множенню взаємно простих чисел

В роботі розглядається метод обчислення циклічних згорток довжиною $N=\prod_{i=0}^{n-1} m_i$, де $(m_i, m_j)=1$, $i \neq j$. Розглядається нове блоково-циклічне представлення згортки за рахунок використання циклічних зсувів у кожному блоці. При такому підході китайська теорема про залишки (КТЗ) не використовується. Метод є ефективним за рахунок використання нескладних перед- та післяобчислень із застосуванням циклічних зсувів. Він дозволяє розпаралелювати обчислення. Отримані апріорні оцінки складності за кількістю операцій множення. Наведені приклади обчислення згорток.

A.N. Tereshchenko, V.K. Zadiraka, A.M. Kudin

Using of Cyclic Shifts for Fast Computation of Cyclic Convolution of Length Equal to Multiplication of Relatively Primes

The computation method of cyclic convolution of two series each of length of $N=\prod_{i=0}^{n-1} m_i$, where $(m_i, m_j)=1$, $i \neq j$ is considered. The new block-cyclic convolution presentation with using of cyclic shifts in each block is proposed. The Chinese Remainder Theorem is not used in this method. The method is effective due to using simple pre- and postcomputations like cyclic shifts. It allows computations in parallel. The number of multiplications in proposed method is given. The examples of convolution computations are presented.

Статья поступила в редакцию 22.06.2011.